AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

13110 Deerpark Drive, Midlothian, Virginia, 23112

Case No. 3:18SW181

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

13110 Deerpark Drive, Midlothian, Virginia, 23112, has a tri-level, single-family residential dwelling, comprised of tan siding and light brown brick, with brick steps and wood handrails leading to a red front door.

located in the Eastern District of Virginia, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B of the attached Affidavit, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §2252A	Possession, Receipt, and Distribution of Child Pornography

The application is based on these facts:

See attached Affidavit, incorporated herein by reference.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Lynette K. Stull, FBI TFO
Printed name and title

Sworn to before me and signed in my presence.

Date: July 24, 2018

/S/
David J. Novak
United States Magistrate Judge
Judge's signature

City and state: Richmond, Virginia

Printed name and title

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Richmond Division

IN THE MATTER OF THE SEARCH OF: 13110 Deerpark Drive, Midlothian, Virginia, 23112	Case No. 3:18 SW 181

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Lynette K. Stull, having been first duly sworn, do hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 13110 Deerpark Drive, Midlothian, Virginia, 23112 (hereinafter, the "SUBJECT PREMISES"), further described in Attachment A, for the things described in Attachment B. Attachments A and B are incorporated herein by reference.

2. I have been a sworn police officer with Chesterfield County Police for over ten years and have been a detective for almost five of those years. I am assigned to Criminal Investigations, Special Victims Unit. I am also currently assigned as a Task Force Officer ("TFO") to the Federal Bureau of Investigation, Richmond Division Child Exploitation Task Force and have been since 2015. I have participated in investigations involving sexual assaults, preferential child molesters, persons who produce, collect, and distribute child pornography, and the importation and distribution of materials relating to the sexual exploitation of children. I

have received training from the FBI in the areas of sexual assaults and child exploitation, and I have reviewed images and videos of child pornography in a wide variety of media forms, including computer media. I have also discussed and reviewed these materials with other law enforcement officers.

3. In the course of my employment as a sworn law enforcement officer, I have participated in the execution of numerous search warrants resulting in the seizure of computers, magnetic storage media for computers, other electronic media, and other items evidencing violations of state and federal laws, including various sections of Title 18, United States Code, Sections 2251, 2252 and 2252A involving child exploitation offenses.

4. I have been deputized as a Special Deputy United States Marshal since July 2015. As a Special Deputy United States Marshal, your Affiant is authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

5. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

6. I have probable cause to believe that the SUBJECT PREMISES contain contraband and evidence of a crime, fruits of a crime, and instrumentalities of violations of: 18 U.S.C. § 2252A (possession, receipt and distribution of child pornography). I submit this application and affidavit in support of a search warrant authorizing a search of the SUBJECT PREMISES, as further described in Attachment A and B, incorporated herein by reference, which is located in the Eastern District of Virginia. Located within the SUBJECT PREMISES to be searched, I seek to seize evidence, fruits, and instrumentalities of the foregoing criminal

violations. I request authority to search the entire SUBJECT PREMISES, including the residential dwelling and any computer, communication devices, and electronic media located therein where the items specified in Attachment A may be found, and to seize all items listed in Attachment B as contraband and instrumentalities, fruits, and evidence of crime.

7. The statements contained in this affidavit are based in part on: information provided by FBI Special Agents, FBI Task Force Agents, and other law-enforcement officers; written reports about this and other investigations that I have received, directly or indirectly, from other law-enforcement agents; information gathered from the service of administrative subpoenas; the results of physical and electronic surveillance conducted by law-enforcement agents; independent investigation and analysis by FBI agents/analysts and computer forensic professionals; and my experience, training, and background as a Special Agent with the Virginia State Police. Because this affidavit is being submitted for the limited purpose of securing authorization for the requested search warrant, I have not included each and every fact known to me concerning this investigation. Instead, I have set forth only the facts that I believe are necessary to establish the necessary foundation for the requested warrant.

DEFINITIONS

8. The following definitions apply to this Affidavit and attachments hereto:

a. "**Erotica**," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, legally obscene or that do not necessarily depict minors in sexually explicit conduct.

b. "**Child Pornography**," as used herein, is defined in 18 U.S.C. § 2256(8) as any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image,

computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

c. **Visual depictions** include undeveloped film and videotape, and data stored on computer disk or by electronic means, which are capable of conversion into a visual image, and data which are capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format. See 18 U.S.C. § 2256(5).

d. **Minor** means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

e. **Sexually explicit conduct** means actual or simulated: (i) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (ii) bestiality; (iii) masturbation; (iv) sadistic or masochistic abuse; or (v) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).

TECHNICAL TERMS

9. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. "**Computer**," as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1) as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

b. "**Computer Server**" or "**Server**," as used herein is a computer that is attached to a dedicated network and serves many users. A web server, for example, is a computer that hosts the data associated with a website. That web server receives requests from a user and delivers information from the server to the user's computer via the Internet. A domain name system ("DNS") server, in essence, is a computer on the Internet that routes communications when a user types a domain name, such as

www.cnn.com, into his or her web browser. Essentially, the domain name must be translated into an Internet Protocol ("IP") address so the computer hosting the web site may be located, and the DNS server provides this function.

c. "**Computer hardware**," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

d. "**Computer software,**" as used herein, is digital information that can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

e. **Wireless telephone**: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

f. **Smartphone** is a portable personal computer with a mobile operating system having features useful for mobile or handheld use. Smartphones, which are typically pocket-sized (as opposed to tablets, which are larger in

measurement), have become commonplace in modern society in developed nations. While the functionality of smartphones may vary somewhat from model to model, they typically possess most if not all of the following features and capabilities: 1) place and receive voice and video calls; 2) create, send and receive text messages; 3) voice-activated digital assistants (such as Siri, Google Assistant, Alexa, Cortana, or Bixby) designed to enhance the user experience; 4) event calendars; 5) contact lists; 6) media players; 7) video games; 8) GPS navigation; 9) digital camera and digital video camera; and 10) third-part software components commonly referred to as "apps." Smartphones can access the Internet through cellular as well as Wi-Fi ("wireless fidelity") networks. They typically have a color display with a graphical user interface that covers most of the front surface of the phone and which usually functions as a touchscreen and sometimes additionally as a touch-enabled keyboard.

g. **SIM card** stands for a "subscriber identity module" or "subscriber identification module," which is the name for an integrated circuit used in mobile phones that is designed to securely store the phone's international mobile subscriber identity (IMSI) number and its related key, which are used to identify and authenticate subscribers on mobile telephony devices (such as mobile phones and computers). It is also possible to store contact information on many SIM cards.

h. **Digital camera**: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

i. **Portable media player**: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

j. **GPS**: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

k. **Tablet**: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, which is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "Wi-Fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

l. The "**Internet**" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

m. "**Internet Service Providers**" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial-up, broadband based access via digital subscriber line ("DSL") or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an "e-mail address," an e-mail mailbox, and

a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an Internet Service Provider ("ISP") over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password.

n. **Internet Protocol address (or simply "IP address")** is a unique numeric address used by computers on the Internet. A typical IP address in IPv4 format looks like a series of four numbers, each in the range 0-255, separated by periods (*e.g.,* 121.56.97.178). Newer IP addresses use the IPv6 format, represented as eight groups of four hexadecimal digits with the groups being separated by colons, for example 2001:0db8:0000:0042:0000:8a2e:0370:7334. Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

o. "The terms "**records**," "**documents**," and "**materials**," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks ("DVDs"), Personal Digital Assistants ("PDAs"), Multi Media Cards ("MMCs"), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

p. **"Website"** consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language ("HTML") and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol ("HTTP").

q. "**P2P**" stands for the expression "peer-to-peer." P2P file sharing is a method of communication available to Internet users through the use of special software. The software enables users to trade digital files through

a network that is formed by directly linking computers together, *i.e.*, "peer to peer." A significant distinction between P2P networks and traditional computer networks is that P2P machines generally communicate directly with each other, rather than through a relatively low number of centrally-based servers. There are a number of widely used P2P programs, including among others BitTorrent, Shareaza, eMule, Ares, and Gnutella. Because of the decentralized nature of P2P networks, they are commonly used to collect and trade illegal files, including, for example, copyright violations involving illegally copied music and movies, as well as child pornography.

r. **"Hash value"** is shorthand for cryptographic hash function value. Hash values are used to identify with extreme precision almost any digital file, including but not limited to a movie file, still image file, word processing document or even the entire contents of a computer hard drive. Hash values are obtained through the use of a mathematical algorithm that maps data of arbitrary size (*e.g.*, a 1 MB image file or a 1 GB movie file) to a bit string of a fixed size (a hash value). The hashing function is designed to be a one-way function, that is, it is infeasible to invert that function and create the original file from the hash value itself. If an original file remains unaltered then the hash value is replicable, *i.e.*, repeatedly hashing the same original file using the same hash algorithm will produce the same value. However, if the original file were to be altered in even a miniscule way, such as cropping a digital photograph to remove even one or two pixels, then the resultant hash value will be completely different. Examples of hash algorithms include the SHA-1, which produces a 40-character hexadecimal formatted hash value (and example of which is "2fd4e1c67a2d28fced849ee1bb76e7391b93eb12"), and the MD5, which produces a 32-character hexadecimal formatted hash value (an example of which is "79054025255fb1a26e4bc422aef54eb4").

BACKGROUND OF THE INVESTIGATION AND PROBABLE CAUSE

10. On February 14, 2018, Special Agent/Child Exploitation Task Force Officer John P. Houlberg, began an investigation into distributors of child pornography over the Internet. On February 14, 2018, between 16:08 PM and 16:15 PM EST, SA Houlberg successfully downloaded child pornography from the dynamic IP address "73.147.221.97," over a P2P network on the Internet using an automated software program used to search P2P networks. This software program is a free version of the P2P program "BitTorrent" that has been configured to

record packet traffic, display geographic locations of IP addresses, and download files from a single source (single source refers to downloading from a single IP address, as opposed to multiple IP addresses as the default P2P configuration for most P2P applications).

11. The BitTorrent network is a very popular and publically available P2P file sharing network. Most computers that are part of this network are referred to as "peers" or "clients". A peer/client can simultaneously provide files to some peers/clients while downloading files from other peers/clients. The BitTorrent network can be accessed by peer/client computers via many different BitTorrent network client (software) programs, examples of which include the BitTorrent client program, uTorrent client program, and Vuze client program, among others. These client programs are publically available and are typically free P2P client software programs that can be downloaded from the Internet.

12. Law enforcement can search the BitTorrent network in order to locate individuals sharing previously identified child exploitation material in the same way a user searches the network. There are BitTorrent network client programs which allow for single-source downloads from a computer at a single IP address, meaning that an entire file or files are downloaded only from a computer at a single IP address as opposed to obtaining the file from multiple peers/clients on the BitTorrent network. This procedure allows for the detection and investigation of those computers involved in sharing digital files of known or suspected child pornography on the BitTorrent network.

13. During the query and/or downloading process from a suspect BitTorrent network client, certain information may be exchanged between the investigator's BitTorrent client program and the suspect client program from which they are querying and/or downloading a

file. This information includes 1) the suspect client's IP address, 2) a confirmation from the suspect client that they have pieces of the file(s) being requested, in whole or in part, and that the pieces of the file(s) is being reported as shared from the suspect client program, and 3) the BitTorrent network client program and version being utilized by the suspect computer. The law enforcement client program has the ability to log this information.

14. Your affiant reviewed the evidence and observed that the automated program successfully achieved a direct connection with IP address 73.147.221.97, on February 14, 2018, between 16:08 PM and 16:15 PM EST. The automated program browsed the BitTorrent files being shared by that IP address during the undercover session on February 14, 2018, at 16:08 PM EST through 16:15 PM EST. Such browsing was conducted using SHA1 hash values.[1] Based on known child pornography SHA1 values, the automated program successfully downloaded 812 BitTorrent files.

15. Your affiant reviewed the downloaded file information and capture logs, which revealed that the download on February 14, 2018, between 16:08 PM EST and 16:15 PM EST, occurred solely from the dynamic IP address 73.147.221.97. Your affiant conducted a check of the American Registry for Internet Numbers ("ARIN") and determined that Comcast Cable Communications, LLC. holds the registration for IP address 73.147.221.97.

16. I reviewed the aforementioned files to determine whether they contained child pornography. Based on my training, experience and review of those images, I determined that there were multiple image files that constituted child pornography, specifically, the lascivious

[1] Previously identified child pornography photographs that are widely circulated on the Internet will, if unaltered, always have the same hash values, which enables investigators to quickly identify other instances of the same offending images.

exhibition of the genitals, as those terms are defined under federal law. Two of the files are described below:

a. **"lsm04-01-039.jpg"** is a color image, depicting two prepubescent females, approximately 8 to 10 years-old. The children are nude and lying on the sand by the water. The first child is lying on her back on what appears to be a leopard print style blanket. She has her knees slightly bent and spread open, exposing her vagina to the camera. She has what appears to be an apple in her right hand. The second child is kneeling, facing towards the other child. Her legs are spread a part and her vagina is exposed for the camera. She has a partially eaten banana in her right hand and the fingers of her left hand are inserted in the mouth of the other child.

b. **"lsm04-03-061.jpg"** is a color image of what appears to be part of the same series of the image described above. This image depicts two prepubescent females, approximately 8 to 10 years old. The children are nude and appear to be outdoors. The children are on their hands and knees on top of a blanket. They are side-by-side and have their heads upside down, facing the camera. Their legs are spread open, exposing their vaginas for the camera. Their vaginas are the focal point of the picture.

17. Based on this information, an administrative subpoena was submitted to Comcast Cable Communication, LLC. on February 15, 2018, requesting subscriber information for the Comcast user-assigned IP address 73.147.221.97, for the aforementioned timeline, during which the files of child pornography were shared.

18. Results from the administrative subpoena revealed the following information about IP address 73.147.221.97, during the aforementioned time frame: (1) the subscriber was "Terry Perry"; (2) the address listed for the account was the SUBJECT PREMISES; and (3) the listed email address was TERRY-PERRY@comcast.net. Comcast records indicated that the dynamic IP address 73.147.221.97, was assigned to the SUBJECT PREMISES beginning on August 25, 2017, through February 16, 2018. Additionally, on July 2, 2018, a second administrative subpoena requesting subscriber information for IP address 73.147.221.97, was submitted to Comcast Cable Communication, LLC. Results received indicated that the IP address 73.147.221.97, was still currently assigned to SUBJECT PREMISIS as of June 29, 2018.

19. Your affiant conducted a search of records of the Virginia Division of Motor Vehicles ("DMV") regarding the names "Terry Perry". Virginia DMV records indicate that Terry Perry has a registered address of the SUBJECT PREMISES. DMV records also indicate that one vehicle is registered to Terry Perry: a 2002 Mercury Sable bearing Virginia registration "KMA4930". The listed address of that vehicle is the SUBJECT PREMISES.

20. A search of the Virginia Employment Commission records for Terry Perry did not return any results.

21. On March 26, 2018, your affiant conducted spot surveillance of the dwelling located at the SUBJECT PREMISES in Chesterfield County. A photograph of the residence is located in Attachment A. Your affiant observed that the residence is a tri-level, single-family residential dwelling. The structure is comprised of tan siding and light brown brick. There are brick steps with wood handrails leading to the front door, which is situated at the center of the house. The front door is red. The mailbox is to the right of the driveway and the numbers

"13110" are affixed below the box. Your affiant observed a silver, Mercury sedan with a Virginia license plate "KMA4930," and a white box truck with a Virginia license plate "VUB7124," parked in the driveway of the residence. Both vehicles are registered to SUBJECT PREMISES.

22. Taken together, the above information indicates that on February 14, 2018, between 16:08 PM EST and 16:15 PM EST hours, a person using a computer(s) located at the SUBJECT PREMISES, in Chesterfield County, was using a computer(s) with the dynamic IP address 73.147.221.97, to download, store, and distribute child pornography files through a file-sharing program on the BitTorrent Network. Based on information provided in this Affidavit, your affiant believes that probable cause exists that child pornography is being stored on a computer(s) in the possession of one or more individuals who resides at the dwelling located at the SUBJECT PREMISES.

23. Because multiple people may share the SUBJECT PREMISES as a residence, it is possible that the SUBJECT PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. While on scene investigators will attempt to use methods and techniques that can identify, or at least narrow down, the device or devices on which the evidence may be found. If, however, those triage techniques are unavailable or unsuccessful and investigators nonetheless determine that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

CHARACTERISTICS OF COLLECTORS OF CHILD PORNOGRAPHY

24. Based upon my knowledge, experience, and training in child pornography

investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the collection of child pornography (hereinafter, "collectors").

25. Collectors may receive sexual stimulation and satisfaction from contact with children, or from having fantasies of children engaged in sexual activity or suggestive poses, or from literature describing such activity.

26. Collectors may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Collectors typically use these materials for their own sexual arousal and gratification. Collectors often have companion collections of child erotica. Child erotica are materials or items that are sexually suggestive and arousing to pedophiles, but which are not in and of themselves obscene or pornographic. Such items may include photographs of clothed children, drawings, sketches, fantasy writings, diaries, pedophilic literature and sexual aids.

27. Collectors who also actively seek to engage in sexual activity with children may use these materials to lower the inhibitions of a child they are attempting to seduce, convince the child of the normalcy of such conduct, sexually arouse their selected child partner, or demonstrate how to perform the desired sexual acts.

28. Collectors almost always possess and maintain their "hard copies" of child pornographic images and reference materials (*e.g.*, mailing and address lists) in a private and secure location. With the growth of the Internet and computers, a large percentage of most collections today are in digital format. Typically, these materials are kept at the collector's

residence for easy access and viewing. Collectors usually place high value on their materials because of the difficulty, and legal and social danger, associated with acquiring them. As a result, it is not uncommon for collectors to retain child pornography for long periods, even for years. Collectors often discard child pornography images only while "culling" their collections to improve their overall quality.

29. Collectors also may correspond with and/or meet others to share information and materials. They may save correspondence from other child pornography distributors/collectors, including contact information like email addresses, and may conceal such correspondence as they do their sexually explicit material.

30. Collectors prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

31. Subscribers to websites that are primarily designed to provide child pornography have a strong likelihood of being collectors of child pornography. This high degree of correlation between subscription and collection behavior has been repeatedly confirmed during nationwide law enforcement initiatives.

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

32. Computers and digital technology have dramatically changed the way in which individuals interested in child pornography interact with each other. It has also revolutionized the methods that individuals will use to interact with and sexually exploit children. Computers serve four functions in connection with child pornography: production, communication, distribution, and storage.

a. **Production.** Child pornographers can now transfer printed photographs into a computer-readable format with a device known as a scanner. Furthermore, with the advent of digital cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera to the computer. The resolution of pictures taken by digital cameras has increased dramatically, meaning the photos taken with digital cameras have become sharper and crisper. Photos taken on a digital camera are stored on a removable memory card in the camera. These memory cards typically store many gigabytes of data, which provides enough space to store thousands of high-resolution photographs. Video camcorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The video files can be easily transferred from the camcorder to a computer.

b. **Distribution and Communication.** A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through digital methods and protocols to anyone with access to a computer and Internet access. Because of the proliferation of commercial services that provide electronic mail service, chat services (*i.e.*, "Instant Messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

c. **Storage.** The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The storage capacity of all electronic media, including but not limited to computer hard drives, is growing constantly These drives can store thousands of images at very high resolution. In addition, there are numerous options available for the storage of computer or digital files. External and internal hard drives with capacities in the terabyte range are not uncommon. Other media storage devices include CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices that are plugged into a port on the computer. It is extremely easy for an individual to take a photo with a digital camera, upload that photo to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices

(CDs and DVDs are unique in that special software must be used to save or "burn" files onto them). Media storage devices can easily be concealed and carried on an individual's person.

33. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

34. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer or external media in most cases.

35. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, *i.e.,* by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, *e.g.,* traces of the path of an electronic communication may be automatically stored in many places (*e.g.,* temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

36. As described above and in Attachment B, this application seeks permission to search for records that might be found in the SUBJECT PREMISES in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

37. *Probable cause.* I submit that if a computer or storage medium is found in the SUBJECT PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data. Depending on a variety of factors, a particular computer could easily not overwrite deleted files with new data for many months, and in certain cases, conceivably ever.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few

examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

38. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the SUBJECT PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration

files, user profiles, e-mail, e-mail address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to engage in a child pornography offense (whether it be to produce, distribute, transport, receive or possess child pornography), the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: 1) data that is evidence of how the computer was used; 2) data that was sent or received; 3) notes as to how the criminal conduct was achieved; 4) records of Internet discussions about the crime; and 5) other records that indicate the nature of the offense.

39. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the SUBJECT PREMISES, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time in the SUBJECT PREMISES could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data in the SUBJECT PREMISES. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

40. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

SPECIFICITY OF SEARCH WARRANT RETURN AND NOTICE REGARDING INITIATION OF FORENSIC EXAMINATION

41. Consistent with the Court's current policy, the search warrant return will list the model(s) and serial number(s) of any and all computers seized at the SUBJECT PREMISES and include a general description of any and all associated peripheral equipment that has been seized. Additionally, the search warrant return will include the total numbers of each type of digital media that has been seized (*e.g.*, "ten (10) 3.5" diskettes; twenty (20) CDs; twenty (20) DVDs; three (3) USB drives; one (1) 256 MB flash memory card," etc.)

42. Moreover, the Government will file a written pleading in this case within one hundred twenty (120) days after the execution of the search warrant notifying the court that the imaging process of digital evidence seized from the target location is complete, and the forensic analysis of computers and media has begun. Such notice will include confirmation that written notice has been provided to the defendant or his counsel informing the defendant that the

forensic examination of evidence seized from him has actually begun. Such notice to the defendant and the Court is not intended to mean, and should not be construed to mean, that the forensic analysis is complete, or that a written report detailing the results of the examination to date will be filed with the Court or provided to the defendant or his counsel. This notice does not create, and is not meant to create, additional discovery rights for the defendant. Rather, the sole purpose of this notice is to notify the defendant that, beyond the simple seizure of his property, a forensic search of that property has actually begun.

CONCLUSION

Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B of this Affidavit, are located at the SUBJECT PREMISES, described in Attachment A. I respectfully request that this Court issue a search warrants for the SUBJECT PREMISES, authorizing the seizure and search of the items described in Attachment B.

Respectfully submitted,

Lynette K. Stull
Task Force Officer
Federal Bureau of Investigation

SEEN

Samuel E. Fishel
Special Assistant United States Attorney

Sworn to me this 24th day of July, 2018

/s/
David J. Novak
United States Magistrate Judge

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Richmond Division

IN THE MATTER OF THE SEARCH OF: 13110 Deerpark Dr., Midlothian, VA 23112	Case No. 3:18 SW 181

ATTACHMENT A

DESCRIPTION OF LOCATION TO BE SEARCHED

The location known as 13110 Deerpark Drive, Midlothian, Virginia, 23112, ("SUBJECT PREMISES") is identified as a tri-level single-family residential dwelling. The structure is comprised of yellow siding. The structure is comprised of tan siding and light brown brick. There are dark wood steps with wood handrails leading to the front door, which is situated at the center of the house. The front door is red. The mailbox is to the right of the driveway and the numbers "13110" are affixed below the box. See below:

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Richmond Division

IN THE MATTER OF THE SEARCH OF: 13110 Deerpark Dr., Midlothian, VA 23112	Case No. 3: 18 SW 181

ATTACHMENT B

EVIDENCE TO BE SEIZED

1. All records relating to violations of 18 U.S.C. §2252A relating to the distribution, receipt and possession of child pornography, including:

   a. any and all visual depictions of minors;

   b. any and all address books, names, and lists of names and addresses of minors;

   c. any and all diaries, notebooks, notes, and any other records reflecting physical contact, whether real or imagined, with minors, and any such items discussing sexual activities with minors;

   d. any and all child erotica, including photographs of children that are not sexually explicit, drawings, sketches, fantasy writings, diaries, and sexual aids;

   e. records and information relating to communications with Internet Protocol addresses 73.147.221.97.

2. Computers or storage media used as a means to commit the violations described above.

3. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

f. evidence of the times the COMPUTER was used;

g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

i. records of or information about Internet Protocol addresses used by the COMPUTER;

j. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

k. contextual information necessary to understand the evidence described in this attachment.

4. Routers, modems, and network equipment used to connect computers to the Internet.

5. Records, information, and items relating to the occupancy or ownership of **13110 Deerpark Dr., Midlothian, VA 23112**, including utility and telephone bills, mail envelopes, or addressed correspondence.

6. Records and information relating to the identity or location of the persons suspected of violating the statutes described above.

7. During the course of the search, law enforcement officials may photograph the searched SUBJECT PREMISES to record the condition thereof and/or the location of items therein.

8. As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

9. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high-speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

10. The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.